SOPHOS

ÉTAT DES RANSOMWARES 2020

Résultats d'une enquête indépendante menée auprès de 5 000 responsables informatiques dans 26 pays différents

Un livre blanc Sophos Mai 2020

Introduction

Des récits d'entreprises paralysées par un ransomware font régulièrement la Une de la presse spécialisée, et les demandes de rançon à six ou sept chiffres sont devenues monnaie courante. Mais ces événements révèlent-ils toute l'histoire ?

Pour comprendre la réalité qui se cache derrière ces gros titres, Sophos a commandé une enquête indépendante auprès de 5 000 responsables informatiques dans 26 pays. Les résultats offrent un tout nouvel éclairage sur ce qui se passe réellement quand un ransomware entre en action. Notre étude révèle le pourcentage d'attaques qui parviennent à chiffrer des données, le nombre de victimes qui paient la rançon, la part du montant de la rançon sur le coût total du nettoyage et l'importance des assurances cybersécurité. Attendez-vous à être surpris.

À propos de l'enquête

Sophos a demandé au cabinet de recherche indépendant Vanson Bourne de réaliser une enquête auprès de 5 000 DSI pour connaître leurs expériences en matière de ransomwares. Sophos n'a joué aucun rôle dans la sélection des répondants et toutes les réponses ont été fournies de manière anonyme. Cette enquête s'est déroulée entre janvier et février 2020.

Les répondants proviennent de 26 pays répartis sur 6 continents :

PAYS	NB DE RÉPONDANTS
Australie	200
Belgique	100
Brésil	200
Canada	200
Chine	200
Colombie	200
République tchèque	100
France	300
Allemagne	300
Inde	300
Italie	200
Japon	200
Malaisie	100

PAYS	NB DE RÉPONDANTS
Mexique	200
Pays-Bas	200
Nigeria	100
Philippines	100
Pologne	100
Singapour	200
Afrique du Sud	200
Espagne	200
Suède	100
Turquie	100
EAU	100
Royaume-Uni	300
États-Unis	500

Au sein de chaque pays, 50 % des répondants sont issus d'entreprises comptant entre 100 et 1 000 employés et 50 % sont issus d'entreprises comptant entre 1 001 et 5 000 employés. Les répondants couvrent un large éventail de secteurs industriels, tant publics que privés.

SECTEUR	NB DE RÉPONDANTS	% DE RÉPONDANTS
IT, technologies et télécoms	979	20 %
Commerce, distribution et transport	666	13 %
Manufacture et production	648	13 %
Services financiers	547	11 %
Secteur public	498	10 %
Services commerciaux et professionnels	480	10 %
Construction et immobilier	272	5 %
Énergie, pétrole/gaz, services publics	204	4 %
Médias, loisirs et divertissement	164	3 %
Autre	542	11 %

Résumé

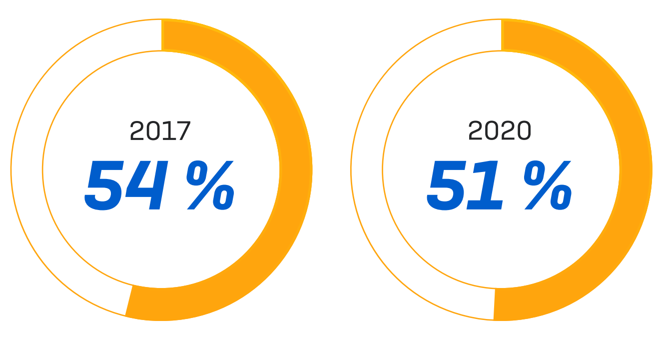
Cette étude apporte un nouvel éclairage sur les expériences des entreprises touchées par un ransomware, notamment :

- **Environ 3/4 des attaques de ransomware aboutissent au chiffrement des données.** 51 % des entreprises ont été touchées par un ransomware au cours de l'année passée. Les cybercriminels ont réussi à chiffrer les données dans 73 % de ces attaques.
- **26 % des victimes dont les données ont été chiffrées les ont récupérées en payant une rançon.** 1 % a payé la rançon, mais n'a pas pu récupérer ses données.
- **94 % des victimes dont les données ont été chiffrées les ont récupérées.** Plus de deux fois plus de victimes les ont récupérées via des sauvegardes (56 %) plutôt qu'en payant une rançon (26 %).
- **Payer la rançon multiplie par deux le coût total d'un ransomware.** Le coût moyen que représente la gestion des dommages causés par les attaques de ransomware les plus récentes (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.) est de 732 520 USD (environ 673 600 €) pour les entreprises qui ne paient pas la rançon, et ce coût passe à 1 448 458 USD (soit à peu près 1 332 000 €) pour les entreprises qui la paient.
- **Malgré le fait qu'il fasse souvent la Une de l'actualité, le secteur public est moins touché par les ransomwares que le secteur privé.** L'an dernier, 45 % des organismes du secteur public ont été touchés par un ransomware, contre une moyenne mondiale de 51 %, avec un maximum de 60 % dans le secteur des médias, des loisirs et du divertissement.
- **1 entreprise sur 5 n'est pas suffisamment protégée par son assurance cybersécurité.** 84 % des répondants ont une assurance cybersécurité, mais seulement 64 % couvrent les attaques de ransomware.
- **L'assurance cybersécurité paie la rançon.** Pour les entreprises bénéficiant d'une assurance couvrant les ransomwares, dans 94 % des cas, lorsque la rançon est payée pour récupérer les données, c'est la compagnie d'assurance qui la paie.
- **Les attaques de ransomware les plus efficaces ciblent les données dans le Cloud public.** 59 % des attaques où les données ont été chiffrées concernaient des données dans le Cloud public. Bien qu'il soit fort probable que les personnes interrogées aient interprété au sens large le terme 'Cloud public', en incluant notamment les services tels que Google Drive et Dropbox et des solutions de sauvegarde telles que Veeam, il est clair que les cybercriminels ciblent les données, peu importe l'endroit où elles se trouvent.

Partie 1 : La prévalence des ransomwares

La moitié des entreprises ont été touchées par un ransomware l'an dernier

51 % des répondants déclarent avoir été touchés par un ransomware au cours de l'année passée. Il semble que le nombre d'attaques ait légèrement diminué par rapport aux années précédentes. En effet, une première enquête commandée par Sophos et publiée en 2017 (échantillon de 1 700 entreprises) révélait que 54 % des répondants avaient été touchés par un ransomware au cours de l'année passée.



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Base : 5 000 répondants (2020), 1 700 répondants (2017).

Cette baisse, bien que bienvenue, est probablement due à un changement de tactique des auteurs de ransomwares plutôt qu'à un intérêt moindre pour ce type d'attaque. Selon les observations des SophosLabs, le marché des ransomwares de type « spray and pray » était très répandu en 2017. Ces attaques étaient lancées en masse et à tout va, ce qui leur permettait de toucher un très grand nombre d'entreprises.

En 2020, la tendance observée est aux attaques de serveurs. Étant hautement ciblées et sophistiquées, ces attaques sont plus complexes à déployer, ce qui pourrait expliquer leur légère baisse. Cependant, elles sont généralement beaucoup plus dangereuses, car elles chiffrent des ressources de haute valeur et peuvent paralyser les entreprises avec des demandes de rançons pouvant aller jusqu'à plusieurs millions d'euros.

Pour les questions subséquentes, si l'entreprise a déclaré plusieurs attaques de ransomwares au cours de l'année passée, nous leur avons demandé de répondre en se basant uniquement sur l'attaque la plus importante.

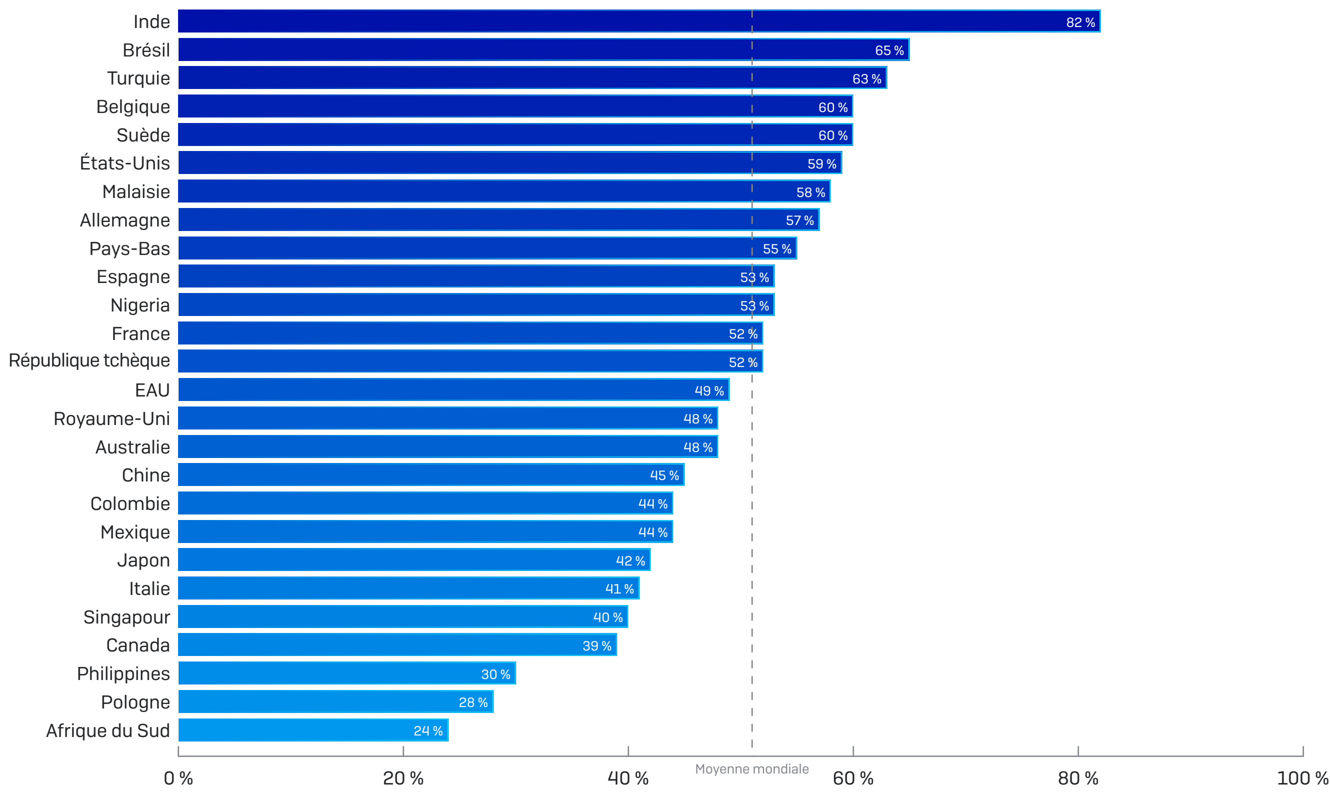
Toutes les tailles d'entreprise sont concernées

Nous observons une faible différence du nombre d'attaques selon la taille de l'entreprise. Un peu moins de la moitié (47 %) des petites entreprises (100-1 000 employés) ont été touchées, tandis qu'un peu plus de la moitié (54 %) des grandes entreprises (1 001-5 000 employés) l'ont été.

Le nombre d'attaques varie selon les pays

L'analyse du nombre d'attaques de ransomware à travers le monde révèle des variations intéressantes. Cela est probablement dû au fait que les cybercriminels concentrent leurs efforts là où se trouvent les plus grandes opportunités de réussite, et aussi au fait que les différents pays ont des niveaux de défense divergents en matière de ransomware.

Pourcentage des entreprises touchées par un ransomware au cours de l'année passée



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Base : 5 000 répondants.

- **L'Inde** (300 répondants) arrive en tête de liste avec 82 % des entreprises déclarant avoir été touchées par un ransomware au cours de l'année passée. Cela n'est pas une grande surprise, car l'hygiène informatique est globalement assez insuffisante en Inde où les technologies piratées prolifèrent, fragilisant les cyberdéfenses et rendant les entreprises plus vulnérables aux attaques.

- **Les Philippines, la Pologne et l'Afrique du Sud** sont les pays ayant été les moins attaqués. Comme nous l'avons vu plus haut, les cybercriminels ont délaissé les attaques de type « spray and pray » pour des attaques de serveurs plus ciblées qui affectent un plus petit nombre d'entreprises, mais avec des demandes de rançon plus élevées. Leurs attaques sont ciblées géographiquement pour s'emparer des opportunités les plus lucratives. Les trois pays les moins attaqués ont un PIB inférieur à celui de nombreux autres pays situés plus haut dans la liste, ce qui peut expliquer pourquoi les cybercriminels leur accordent moins d'attention.

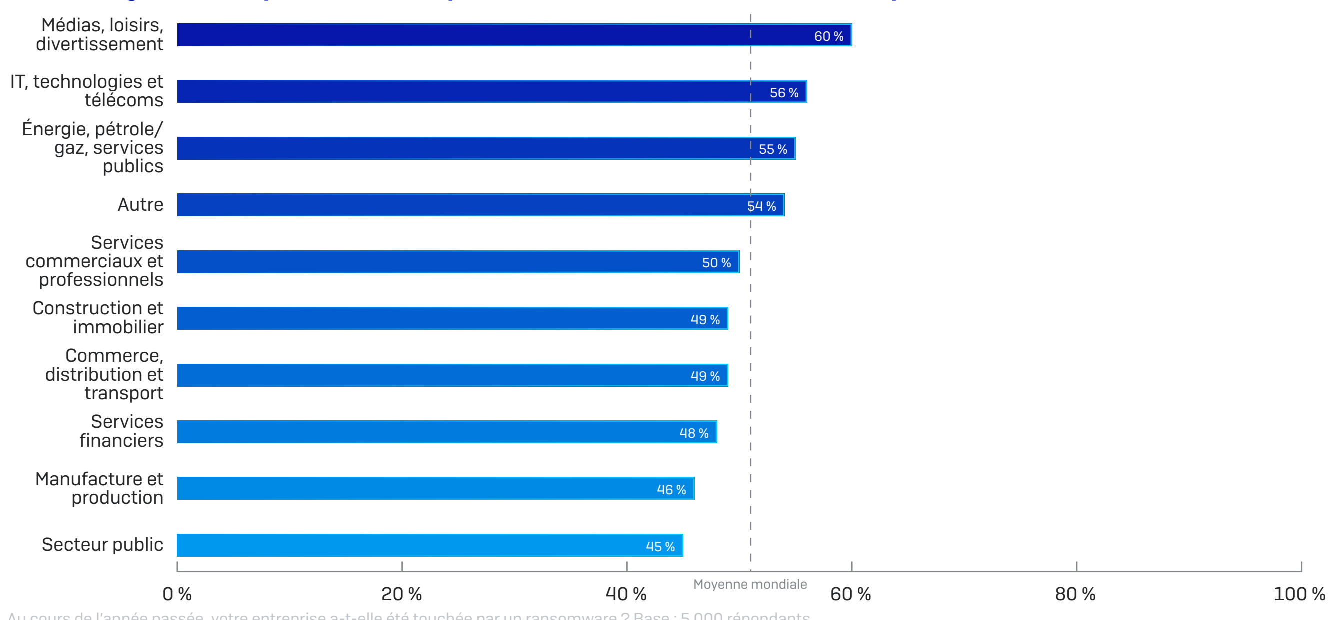
- Le désintérêt pour les méthodes « spray and pray » à la faveur d'attaques ciblant les proies les plus lucratives a probablement contribué à la réduction notable des ransomwares en **Afrique du Sud**. En effet, dans notre enquête de 2017, 54 % des répondants sud-africains avaient déclaré avoir été touchés par un ransomware au cours de l'année écoulée, mais ce chiffre est aujourd'hui descendu à 24 %, soit une baisse de plus de 50 % des cas.

- **Le Canada** (200 répondants) fait état d'un nombre étonnamment faible d'attaques de ransomware. En tant que pays occidental avancé, il pourrait être considéré comme une cible lucrative, pourtant seulement 39 % des répondants déclarent avoir été attaqués. C'est 20 % de moins que les États-Unis voisins, où 59 % des personnes interrogées ont été touchées par un ransomware. Il se peut que le Canada profite du fait d'être dans l'ombre des États-Unis, où toute l'attention des cybercriminels se concentre. Dans le même temps, les répondants canadiens sont très attentifs à la question et 68 % des entreprises non touchées s'attendent à une attaque future.

Le secteur public a subi le moins d'attaques

Oui, vous avez bien lu. Le secteur public a déclaré moins d'attaques que tous les autres secteurs. Le secteur des médias, loisirs et divertissement est en fait celui qui enregistre le plus haut niveau d'attaques (60 %), suivi de près par le secteur IT, technologies et télécoms (56 %).

Pourcentage des entreprises touchées par un ransomware au cours de l'année passée



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Base : 5 000 répondants.

Cela peut sembler surprenant à première vue, car la presse publie régulièrement des récits d'hôpitaux ou d'organismes gouvernementaux attaqués par un ransomware. Toutefois, notre enquête révèle que ces gros titres donnent une image faussée de la réalité.

Dans de nombreux pays, les organismes du secteur public ont pour obligation de déclarer toute attaque de ransomware. Ce qui n'est souvent pas le cas pour les entreprises du secteur privé, qui peuvent ainsi choisir de passer une attaque sous silence. Les raisons peuvent être multiples : éviter d'inquiéter les clients, ne pas ternir leur réputation ou éviter d'être identifié comme une cible facile par d'autres attaquants.

Ces résultats sont corroborés par les recherches effectuées par Sophos sur le ransomware SamSam. En collaboration avec l'organisme de surveillance des cryptomonnaies Neutrino, Sophos avait suivi les gains engrangés par SamSam, ce qui leur avait permis de découvrir de nombreux paiements et victimes qui ne s'étaient jamais signalés. Cette étude a révélé que les victimes du secteur privé étaient celles qui avaient le plus souffert de SamSam.

Partie 2 : L'impact des ransomwares

Les 3/4 des attaques de ransomwares aboutissent au chiffrement des données

Traditionnellement, pour être fructueuse une attaque de ransomware se compose de 3 volets : le chiffrement des données, l'obtention du paiement de la rançon et le déchiffrement des données. Dans près de 3/4 des attaques (73 %), les cybercriminels sont parvenus à chiffrer les données.

Il est toutefois encourageant de constater que dans un peu moins de 1/4 des cas (24 %), l'attaque a été stoppée avant que les données ne puissent être chiffrées. Il semble que les technologies anti-ransomware aient un réel impact sur le taux de réussite de ces attaques.



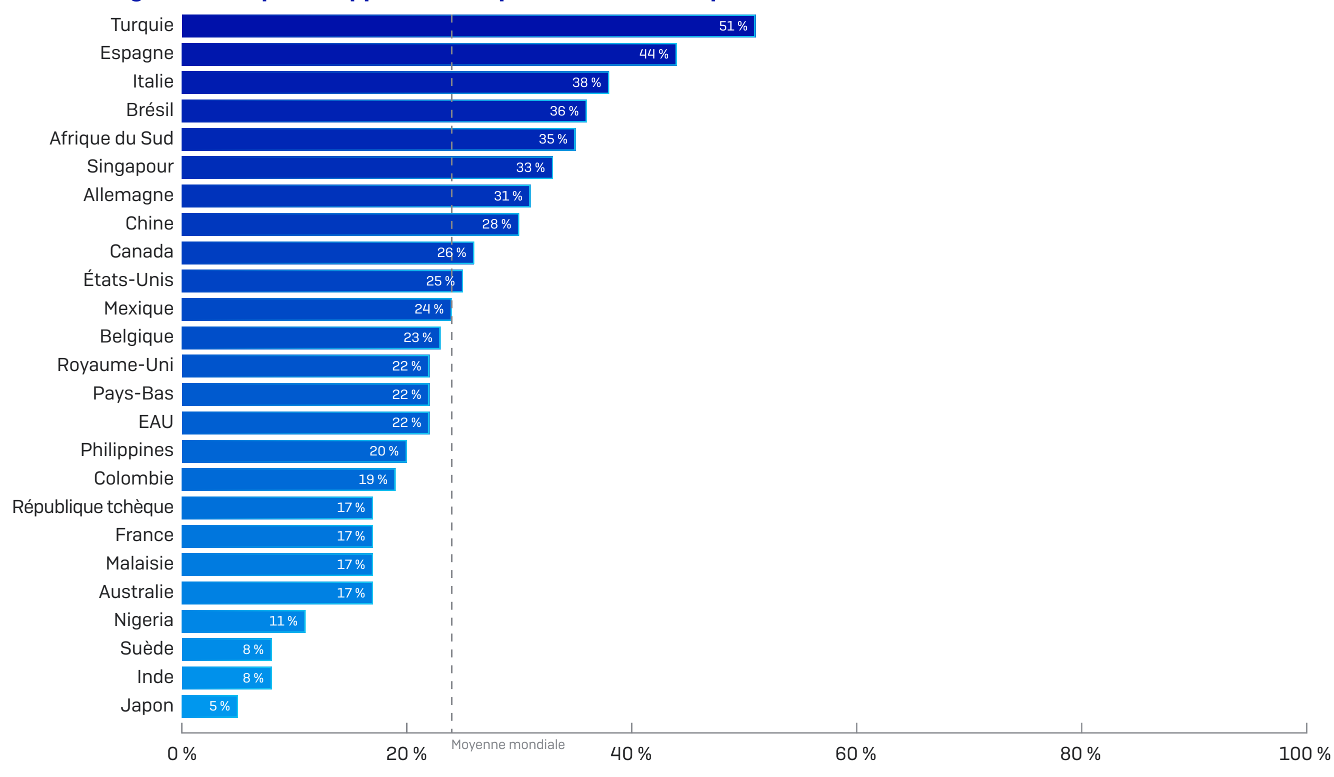
Un résultat intéressant de l'enquête est que 3 % des victimes ont déclaré que leurs données n'avaient pas été chiffrées, mais qu'elles avaient tout de même été rançonnées. Ce type d'attaque est particulièrement répandu au Nigeria, ainsi qu'en Colombie, en Afrique du Sud, en Chine, en Pologne, en Belgique et aux Philippines.

On pourrait d'ailleurs plutôt parler d'extorsion que de rançon. Mais au-delà de la sémantique, il est important de garder à l'œil ce type d'attaque, car les escrocs cherchent de plus en plus des moyens de gagner de l'argent sans avoir à chiffrer et à déchiffrer les fichiers.

Les attaques sont plus susceptibles de réussir au Japon

Sur le plan national, c'est le Japon qui réussit le moins à stopper les attaques, avec 95 % aboutissant au chiffrement des données. À l'inverse, en Turquie, la moitié des attaques (51 %) ont été stoppées avant que les données ne puissent être chiffrées. Ces variations peuvent s'expliquer par une sensibilisation différente selon les pays à la prévalence des ransomwares et à la probabilité d'être touché, ce qui pourrait entraîner des niveaux de protection différents contre les ransomwares.

Pourcentage des attaques stoppées avant que les données ne puissent être chiffrées

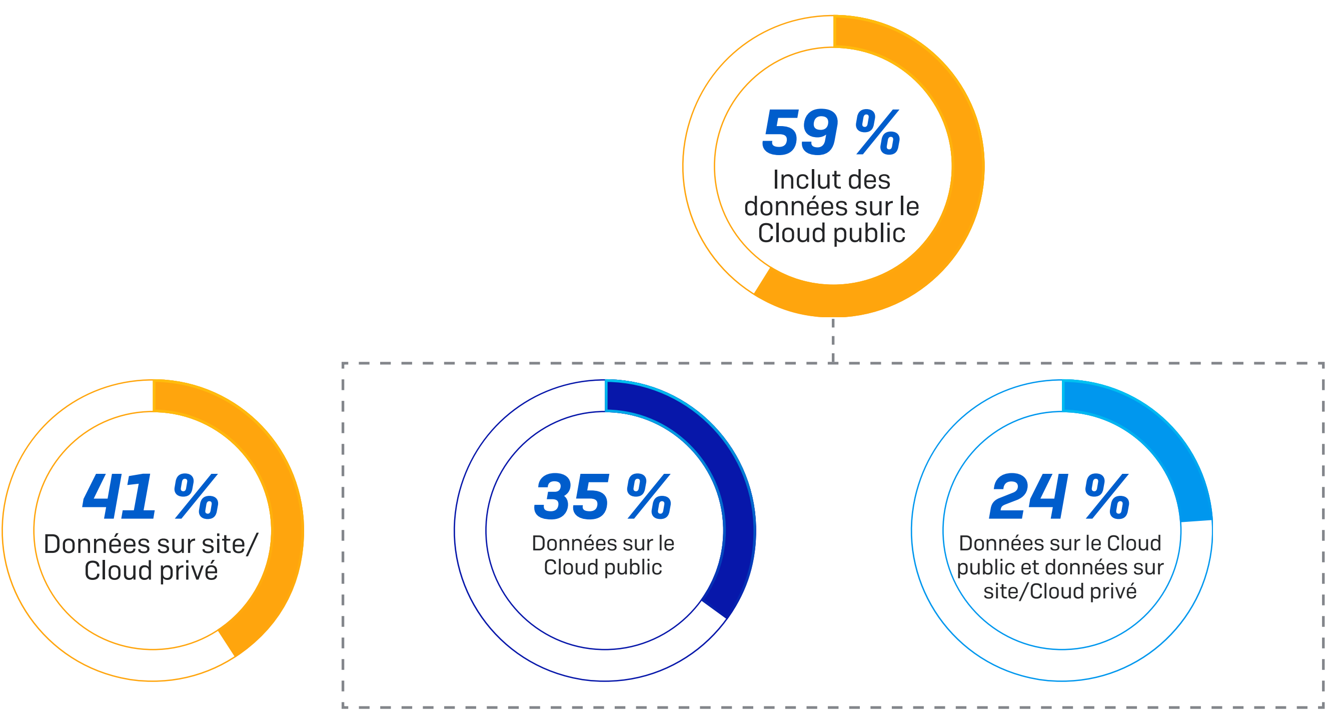


Pourcentage des répondants ayant répondu « Non, l'attaque a été stoppée avant que les données n'aient pu être chiffrées » à la question : Lors de l'attaque de ransomware la plus importante, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? La question n'était visible qu'aux répondants ayant déclaré avoir été touchés par un ransomware au cours de l'année passée. Base : 2 538 répondants.

La Pologne a été retirée de ce graphique, car la base est inférieure à 30 répondants, et les Philippines ont une base de tout juste 30 répondants.

Les données dans le Cloud public sont les cibles de choix

Nous avons demandé aux 73 % de répondants dont les données ont été chiffrées quels types de données avaient été affectés. Pour 41 %, le ransomware a chiffré des données locales ou dans le Cloud privé, tandis que pour 35 % l'attaque a uniquement visé des données dans le Cloud public. Pour 24 %, il s'agissait d'un mélange entre les deux. Au total, près de 6 attaques réussies sur 10 (59 %) incluent des données dans le Cloud public.



Lors de l'attaque de ransomware la plus importante, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Les réponses viennent de répondants dont les données de l'entreprise ont été chiffrées lors de l'attaque de ransomware la plus récente. Base : 1 849 répondants.

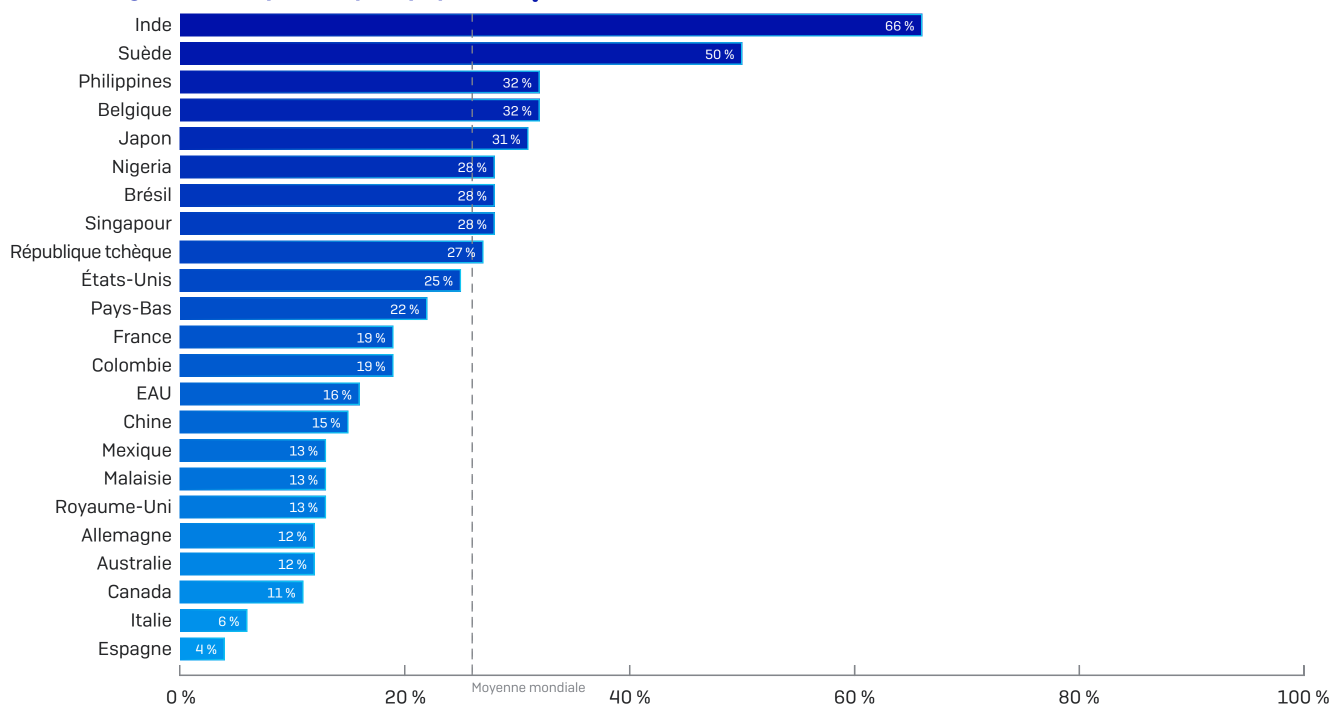
Mais attention : il est probable que les personnes interrogées aient interprété au sens large le terme 'Cloud public', incluant des services tels que Google Drive et Dropbox et des solutions de sauvegarde telles que Veeam, plutôt qu'uniquement des services Cloud de type AWS, Azure et Alibaba. Néanmoins, il y a un point important à retenir : aucune donnée n'est en sécurité et il vous incombe de vous assurer que les données stockées dans le Cloud sont aussi bien protégées et sauvegardées que les données stockées sur site.

26 % des victimes de ransomwares ont récupéré leurs données en payant la rançon

26 % des entreprises dont les données ont été chiffrées les ont récupérées en payant la rançon. En revanche, 1 % des entreprises dont les données ont été chiffrées ont payé la rançon, mais n'ont pas récupéré leurs données. Ainsi, au total, 95 % des entreprises ayant payé la rançon ont vu leurs données restaurées (soit 473 des 496 entreprises ayant payé la rançon).

En ce qui concerne le paiement des rançons, nous constatons des variations régionales notables. En Inde, 2 entreprises sur 3 (66 %) ont payé la rançon pour récupérer leurs données, tandis que 29 % ont utilisé des sauvegardes. À l'inverse, en Espagne, seuls 4 % ont payé la rançon, tandis que 72 % ont restauré leurs données à partir de sauvegardes.

Pourcentage des entreprises ayant payé la rançon



Pourcentage des répondants ayant répondu « Oui, nous avons payé la rançon » à la question : Lors de l'attaque de ransomware la plus importante, votre entreprise a-t-elle récupéré ses données ? La question n'était visible qu'aux répondants ayant déclaré avoir subi une attaque de ransomware ayant abouti au chiffrement des données. Base : 1 849 répondants.

Veuillez noter que nous avons retiré les Philippines, l'Afrique du Sud, la Pologne et la Turquie du graphique, car ils avaient tous une base de 30 répondants ou moins pour cette question.

94 % des entreprises ont récupéré leurs données

Bien que 73 % des attaques de ransomware parviennent à chiffrer les données, la bonne nouvelle est que 94 % des entreprises touchées ont réussi à les récupérer.

Comme nous l'avons vu, 26 % des victimes de ransomwares ont récupéré leurs données en payant la rançon. Cependant, plus du double (56 %) ont restauré leurs données en utilisant des sauvegardes. Les 12 % restants ont déclaré les avoir récupérées par d'autres moyens.



La taille de l'entreprise a une incidence sur le coût de la remédiation

Sans surprise, l'enquête a confirmé que le coût de remédiation d'une attaque de ransomware est plus élevé pour les grandes entreprises.

Coût moyen pour remédier à une attaque de ransomware



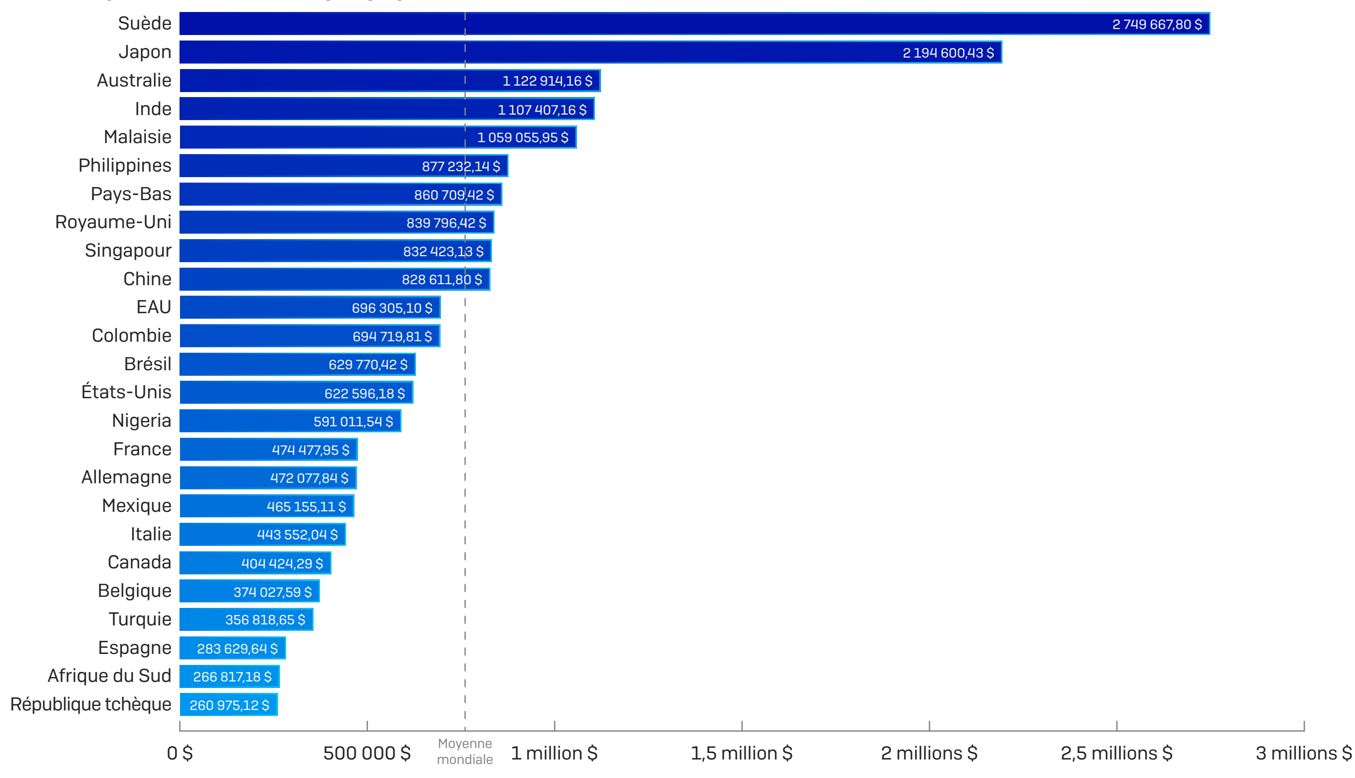
Quel était le montant approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus récente (en prenant en compte les pannes, temps de travail sacrifié, coûts du matériel et du réseau, manque à gagner, rançons payées, etc.) ? La question n'était visible qu'aux répondants ayant déclaré avoir été touchés par un ransomware au cours de l'année passée. Base : 2 538 répondants.

Le coût moyen que représente la gestion des dommages causés par les attaques de ransomware les plus récentes (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.) est de 761 106 USD (env. 695 274 €). Pour les entreprises de 100 à 1 001 employés, le coût moyen était de 505 827 USD (env. 462 075 €), et pour les entreprises de 1 001 à 5 000 employés il était de 981 140 USD (env. 896 276 €).

Le coût des ransomwares varie selon les pays

Ce qui est surprenant, cependant, est la variation du coût de la remédiation entre les pays étudiés. La Suède et le Japon, en particulier, font état de coûts considérablement plus élevés que tous les autres pays. En revanche, l'Afrique du Sud et la République tchèque ont les coûts de remédiation les plus bas. Nous avons exclu la Pologne de ce graphique, car elle avait une base de moins de 30 répondants.

Coût moyen de remédiation par pays



Quel était le montant approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus récente (en prenant en compte les pannes, temps de travail sacrifié, coûts du matériel et du réseau, manque à gagner, rançons payées, etc.) ? La question n'était visible qu'aux répondants ayant déclaré avoir été touchés par un ransomware au cours de l'année passée. Base : 2 538 répondants.

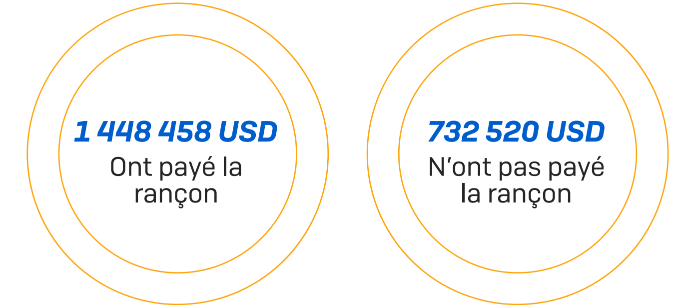
Une des raisons possibles à cette variation est le coût de la main-d'œuvre dans les différents pays. La Suède et le Japon sont typiquement des pays où les salaires sont plus élevés, de sorte que les coûts des heures de travail nécessaires pour remédier à l'attaque s'additionneront rapidement. À l'inverse, l'Afrique du Sud et la République tchèque sont des pays où le coût de la main-d'œuvre est généralement plus faible.

Parmi tous les pays interrogés, nous avons vu que la Suède est le deuxième pays le plus enclin à payer la rançon, juste après l'Inde. Toutefois, contrairement à l'Inde, elle a aussi de hauts salaires à payer, ce qui la pénalise doublement.

Payer la rançon double les coûts

L'une des conclusions les plus intéressantes de l'enquête est que le fait de payer la rançon double quasiment le coût total de la remédiation par rapport à ceux qui choisissent de ne pas la payer ou de récupérer leurs données à l'aide de sauvegardes ou par d'autres moyens. Ne pas payer la rançon a ainsi deux effets : non seulement vous serez satisfait de ne pas avoir donné d'argent à des criminels, mais cela vous permet également d'économiser de l'argent à long terme.

Coût moyen pour remédier à une attaque de ransomware



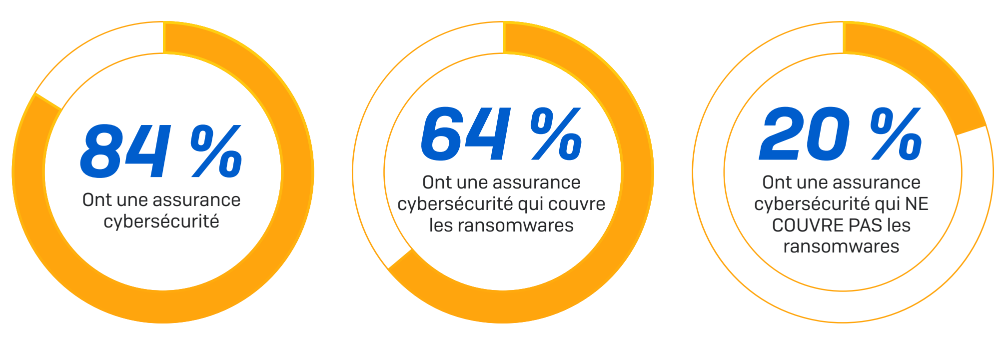
Lors de l'attaque de ransomware la plus importante, votre entreprise a-t-elle récupéré ses données ? Les résultats ne représentent que les répondants dont les données de l'entreprise ont été chiffrées lors de l'attaque de ransomware la plus récente. Base : 1 849 répondants. **Ont payé la rançon** combine les réponses « Oui, nous avons payé la rançon » et « Non, bien que nous ayons payé la rançon ». **N'ont pas payé la rançon** combine les réponses « Oui, nous avons utilisé des sauvegardes pour restaurer les données », « Oui, nous avons utilisé d'autres moyens pour récupérer nos données » et « Non, nous n'avons pas payé la rançon ».

Cela peut sembler contre-intuitif : si vous avez payé la rançon, pourquoi cela vous coûte-t-il plus cher ? Même si vous avez payé la rançon, il reste encore beaucoup de choses à faire pour récupérer vos données. En réalité, les coûts engendrés pour récupérer vos données et revenir à la normale seront probablement similaires, que vous les récupériez auprès des criminels ou grâce à vos sauvegardes. Mais si vous payez la rançon, vous rajoutez une somme colossale à la facture.

Partie 3 : L'importance des assurances

1 entreprise sur 5 déplore des lacunes dans son assurance cybersécurité

Recourir à une assurance cybersécurité est devenu la norme, avec 84 % des entreprises déclarant en avoir souscrit une. Toutefois, seulement 64 % ont une assurance qui couvre les ransomwares. Cela signifie que 1 entreprise sur 5 (20 %) paie une assurance cybersécurité qui ne la couvre pas en cas d'attaque de ransomware.



Votre entreprise a-t-elle une assurance cybersécurité qui couvre les attaques de ransomwares ? Base : 5 000 répondants.

Étant donné que 51 % des entreprises ont été touchées par un ransomware au cours de l'année passée, et que le coût moyen de remédiation s'élève à 761 106 USD (env. 695 274 €), les entreprises devraient fortement s'interroger sur la valeur des assurances qui excluent les ransomwares.

Assurance cybersécurité par pays

Pays	Ont une assurance cybersécurité	Ont une assurance cybersécurité qui couvre les ransomwares
Inde	94 %	80 %
Chine	94 %	82 %
Turquie	93 %	57 %
Afrique du Sud	91 %	70 %
États-Unis	90 %	75 %
Suède	89 %	75 %
Malaisie	89 %	57 %
Royaume-Uni	88 %	70 %
Italie	88 %	68 %
EAU	85 %	55 %
Brésil	85 %	68 %
Canada	84 %	62 %
Espagne	83 %	70 %
Australie	82 %	65 %
Mexique	82 %	61 %
Philippines	81 %	49 %
France	81 %	61 %
Belgique	81 %	69 %
République tchèque	80 %	48 %
Colombie	77 %	57 %
Allemagne	77 %	50 %
Pays-Bas	76 %	64 %
Japon	75 %	58 %
Singapour	74 %	56 %
Pologne	71 %	44 %
Nigeria	70 %	45 %

0 % 20 % 40 % 60 % 80 % 100 %

Votre entreprise a-t-elle une assurance cybersécurité qui couvre les attaques de ransomwares ? Base : 5 000 répondants.

Ce graphique présente les données par pays. En bleu, le pourcentage d'entreprises ayant une assurance cybersécurité et en orange, le pourcentage ayant une assurance couvrant les ransomwares. Ce que nous devons considérer ici, ce sont à la fois les chiffres absolus pour chaque ligne, mais aussi l'écart entre les deux lignes pour chaque pays.

L'Inde arrive en tête de liste des entreprises ayant une assurance cybersécurité et se situe au deuxième rang (80 %) des entreprises dont l'assurance couvre les ransomwares. Cela parait logique, étant donné qu'il s'agit du pays le plus attaqué par les ransomwares.

Selon les résultats, la Turquie est le troisième pays le plus attaqué par des ransomwares. Toutefois, si elle se classe au troisième rang des pays pour les assurances cybersécurité (93 % des entreprises sont couvertes), elle présente également l'un des plus grands écarts entre les deux lignes, avec seulement 57 % des entreprises protégées contre les attaques de ransomware.

Bien que la Chine ait un taux d'attaques de ransomware inférieur à la moyenne (45 % l'année dernière), elle a, avec l'Inde, le niveau d'assurance cybersécurité le plus élevé (94 %) ainsi que le niveau d'assurance couvrant les ransomwares le plus élevé (82 %). C'est en effet le pays qui présente le plus petit écart entre les deux lignes parmi les 26 pays étudiés.

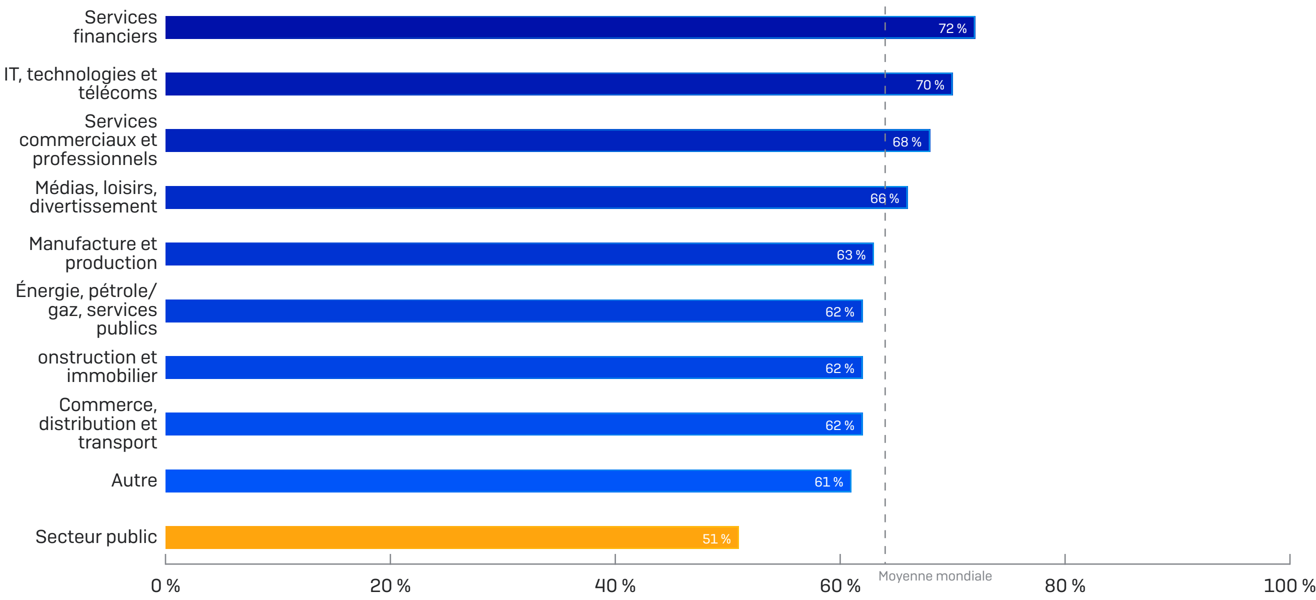
L'Allemagne est une exception intéressante. Il est surprenant de voir une économie développée avec un niveau d'assurance aussi bas (77 %), ainsi qu'un des niveaux les plus bas de protection contre les ransomwares (50 %). L'Allemagne a subi plus d'attaques de ransomware que la moyenne des pays (57 % des entreprises ont été touchées au cours de l'année passée), ce qui rend ce faible taux d'assurance encore plus surprenant.

Le secteur public supporte les coûts les plus importants

Bien que nous ayons constaté que le secteur public est celui le moins exposé aux ransomwares, il est aussi celui qui supporte les coûts les plus lourds.

En moyenne, 64 % des entreprises ont une assurance qui couvre les ransomwares. Le secteur des services financiers présente le taux de couverture le plus élevé (72 %), probablement en raison de sa nature qui en fait une cible lucrative privilégiée. Il est talonné par le secteur IT, télécoms et technologies avec 70 % des entreprises couvertes.

Une assurance cybersécurité qui couvre les ransomwares

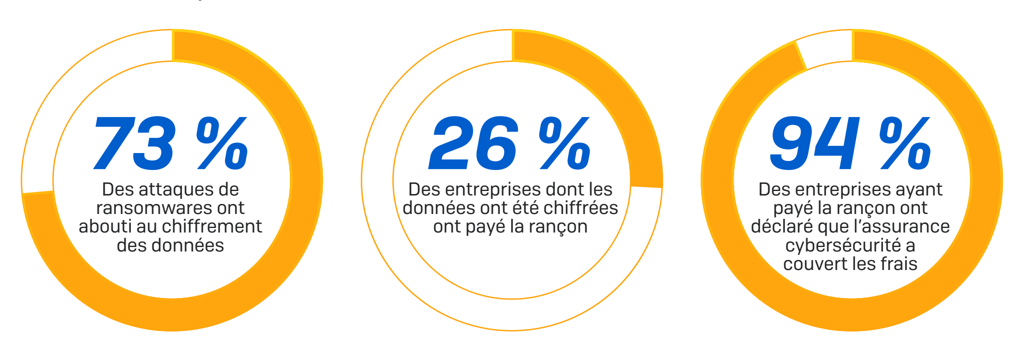


Votre entreprise a-t-elle une assurance cybersécurité qui couvre les attaques de ransomwares ? Base : 5 000.

Les organismes du secteur public sont toutefois très en retard sur leurs homologues du privé. Seuls 51 % ont une assurance qui prend en charge les coûts d'une attaque de ransomware, soit 10 % de moins que le secteur qui le talonne dans la liste. Ce faible taux de protection pourrait s'expliquer par le coût de l'assurance. Le manque de fonds du secteur public est une réalité dans le monde entier et il est fréquent que les budgets ne permettent pas de financer une assurance. Mais dans tous les cas, si une attaque parvient à franchir leurs défenses, cette économie n'aura été que de court terme.

Assurance cybersécurité et paiement des rançons

Examinons maintenant le rôle de l'assurance cybersécurité dans le paiement des rançons. Comme nous l'avons vu, 73 % des attaques de ransomwares aboutissent au chiffrement des données. Parmi les entreprises dont les données ont été chiffrées, 26 % ont déclaré avoir payé la rançon pour les récupérer.



Mais en y regardant de plus près, on se rend compte que dans 94 % des cas où la rançon a été payée, c'est l'assurance cybersécurité qui a pris en charge le paiement. Et, comme nous l'avons constaté plus haut, payer la rançon double le coût total du nettoyage.

Partie 4 : Techniques d'attaque des ransomwares

Nous avons demandé aux entreprises qui ont été touchées par un ransomware l'an dernier comment l'attaque était entrée dans l'entreprise. En tête de liste avec 29 % des attaques, on retrouve les fichiers téléchargés/emails avec pièce jointe malveillante. En second, avec 21 % des attaques, on retrouve les attaques à distance des serveurs.

COMMENT LE RANSOMWARE EST ENTRÉ DANS L'ENTREPRISE	NB D'INCIDENTS	% D'INCIDENTS
Via un fichier téléchargé/email avec PJ malveillante	741	29 %
Via une attaque à distance du serveur	543	21 %
Via un email avec pièce jointe malveillante	401	16 %
Instances de Cloud public mal configurées	233	9 %
Via le protocole RDP (Remote Desktop Protocol)	221	9 %
Via un prestataire avec qui nous collaborons	218	9 %
Via une clé USB/support amovible	172	7 %
Autre	0	0 %
Ne sait pas	9	0
Total	2 538	100 %

Comment le ransomware est-il entré dans votre entreprise ? Question posée aux répondants ayant déclaré avoir été touchés par un ransomware au cours de l'année passée. Base : 2 538 répondants.

Ces données mettent en relief une information importante : il n'y a pas qu'un seul vecteur d'attaque principal. En effet, les cybercriminels déploient tout un éventail de techniques d'attaque pour se donner toutes les chances de percer les défenses. Lorsqu'une technique échoue, ils passent à la suivante, et ce jusqu'à ce qu'ils trouvent enfin une faille.

Ces données démontrent la nécessité de mettre en place une défense multicouche qui couvre vos postes, vos serveurs, les instances du Cloud public, la messagerie, la passerelle réseau et la chaîne d'approvisionnement. Se concentrer sur une seule technologie est le plus sûr moyen d'être infecté.

Recommandations

Cette enquête confirme que les ransomwares restent bel et bien une menace pour les entreprises aujourd'hui. Elle offre également des recommandations pour réduire le risque d'être pris en otage :

1. **Partez du principe que vous serez un jour touché.** Les ransomwares ne font pas de distinction : chaque entreprise est une cible, peu importe sa taille, son secteur ou sa zone géographique. Planifiez votre stratégie de cybersécurité en partant du principe que vous serez un jour touché par une attaque.
2. **Investissez dans une technologie anti-ransomware pour stopper le chiffrement non autorisé.** 24 % des répondants touchés par un ransomware ont pu arrêter l'attaque avant que les données ne puissent être chiffrées.
3. **Protégez les données, en tous lieux.** Près de 6 attaques de ransomware sur 10 parvenues à chiffrer des données incluent des données dans le Cloud public. Votre stratégie doit inclure la protection des données dans le Cloud public, le Cloud privé et sur site.
4. **Faites des sauvegardes régulières et gardez-les hors site et hors ligne.** 56 % des entreprises dont les données ont été chiffrées les ont restaurées à l'aide de sauvegardes. Pour restaurer vos données, il est beaucoup moins coûteux d'utiliser des sauvegardes que de payer la rançon.
5. **Assurez-vous que votre assurance cybersécurité couvre les attaques de ransomwares.** Assurez-vous que vous êtes entièrement couvert si le pire devait se produire.
6. **Déployez une défense par couches.** Les auteurs des ransomwares utilisent un large éventail de techniques pour contourner vos défenses ; lorsqu'une d'entre elles est bloquée, ils passent à la suivante jusqu'à ce qu'ils trouvent la faille dans votre défense. Vous devez vous protéger contre tous les vecteurs d'attaque.

Présentation de Sophos Intercept X Endpoint

Les auteurs de ransomwares combinent des techniques d'attaque sophistiquées avec du pilotage manuel. Sophos Intercept X Endpoint vous dote des technologies de protection avancées dont vous avez besoin pour neutraliser toute la chaîne d'attaque, notamment :

- **Restauration des données chiffrées** - CryptoGuard bloque le chiffrement non autorisé des fichiers, puis les restaure vers leur état d'origine sain en quelques secondes.
- **Protection anti-exploit** - Elle détecte et bloque plus de deux dizaines de techniques d'exploits (utilisées pour télécharger et installer des malwares) afin d'empêcher les attaquants de pénétrer votre réseau.
- **Protection optimisée par IA** – Le moteur de Deep Learning de Sophos prévient de manière prédictive un plus grand nombre d'attaques, et présente moins de faux positifs que tout autre logiciel de sécurité.
- **Protection contre le vol d'identifiants** - Elle empêche les hackers de mettre la main sur vos identifiants, bloquant les accès système non autorisés et l'élévation des privilèges admin.

Pour en savoir plus et démarrer une démo en ligne instantanée, RDV sur

www.sophos.fr/intercept-x

À propos de Vanson Bourne

*Vanson Bourne est un cabinet d'études de marché indépendant spécialisé dans le secteur des technologies. Sa réputation d'analyste solide et crédible repose sur des principes de recherche rigoureux et sur sa capacité à solliciter l'avis des décideurs de haut niveau dans les domaines techniques et commerciaux, dans tous les secteurs d'activité et sur l'ensemble des marchés dominants. Visitez leur site Web*www.vansonbourne.com

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

200427 WPFR (DD)

SOPHOS